PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS
Veterans Affairs Center Office
Veterans Affairs Center for Innovation
And
Veterans Health Administration Innovation Program

Spinal Cord Injury Environmental Control Unit Implementation

Date: June 16, 2014
TAC-14-16642
PWS Version Number: 1.0

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), VA Center for Innovations (VACI), and the Veterans Health Administration (VHA) Innovation Program is to field, fund, and foster ideas that benefit Veteran's health. The program allows mission critical healthcare innovations to emerge from the field and industry. These ideas, along with those from leadership, are matured through a collaborative constructive review by communities of interest, and are piloted in a safe harbor for innovation. Innovations that are proven and vetted from business and technical perspectives will have a pathway for organizational acceptance and diffusion.

This requirement is for the purchase and installation of environmental control units (ECUs) for spinal cord injury patients, as well as to provide dual mounting for sites that already have individual patient televisions mounted from articulating arms.

Spinal cord injury patients with limited functionality do not have the capability to control their surroundings. The ECUs will provide an increased quality of patient care as well as patient safety.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement (PWS), the Contractor shall comply with the following:

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
3. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
4. Department of Veterans Affairs (VA) Directive 0710, "Personnel Suitability and Security Program," May 18, 2007
5. VA Directive 6102, "Internet/Intranet Services," July 15, 2008
6. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
7. OMB Circular A-130, "Management of Federal Information Resources," November 28, 2000
8. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
9. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
10. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
11. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
12. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
13. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," September 20, 2012
14. VA Handbook 6500.1, "Electronic Media Sanitization," March 22, 2010
15. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)", January 6, 2012
16. VA Handbook 6500.3, "Certification and Accreditation of VA Information Systems," November 24, 2008
17. VA Handbook, 6500.5, "Incorporating Security and Privacy in System Development Lifecycle" March 22, 2010

18. VA Handbook 6500.6, "Contract Security," March 12, 2010
19. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
20. VA Directive 6300, Records and Information Management, February 26, 2009
21. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
22. OMB Memorandum, "Transition to IPv6", September 28, 2010

3.0 SCOPE OF WORK

The Contractor shall provide all necessary services and materials to configure, install and test Environmental Control Units for spinal cord injury patient beds as specified by each facility herein.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be a 12-month base period, with one 12-month option period.

Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO). There are 10 Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six are set by a day of the week and month:

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed at the following VA facilities:

Base Period
1. James A. Haley VAMC, Tampa, FL 2. Louis Stokes VAMC, Cleveland ,OH

Option Period 1
1. VA Long Beach Healthcare System, Long Beach, CA 2. VA Palo Alto Healthcare System, Palo Alto, CA 3. Saint Louis Health Care System, St. Louis, MO 4. VA San Diego Health Care System, San Diego, CA 5. Hampton VAMC, Hampton, VA

4.3 TRAVEL

The Government anticipates travel under this effort to perform the tasks associated with the effort. Include all estimated travel costs in your firm-fixed price line items. These costs will not be directly reimbursed by the Government. The total estimated number of trips in support of this effort is identified below. Anticipated locations include the following, estimated at a maximum of five days in duration for up to three people to each site.

LOCATION	TRIPS	DURATION DAYS
James A. Haley VAMC, Tampa, FL - Base Period	**12**	5
Louis Stokes VAMC, Cleveland, OH - Base Period	**4**	5
VA Long Beach Healthcare System, Long Beach, CA – Option Period 1	**2**	5
VA Palo Alto Healthcare System, Palo Alto, CA – Option Period 1	**2**	5
Saint Louis Health Care System, St. Louis, MO - Option Period 1	**2**	5
VA San Diego Health Care System, San Diego, CA - Option Period 1	**2**	5
Hampton VAMC, Hampton VA - Option Period 1	**9**	5

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 PROJECT KICK-OFF MEETING

The Contractor shall hold a Project Kick-Off Meeting with an Integrated Project Team (IPT) consisting of all key stakeholders including the Contracting Officer's Representative (COR) and Contracting Officer (CO) within 10 calendar days of contract award. At the Project Kick-Off Meeting, the Contractor shall present the details of its intended approach, work plan, Contractor Project Management Plan (CPMP) and project schedule, including deliverable dates, for review and approval by the VA Program Manager (PM) and COR. The Contractor shall provide a Project Kick-Off Meeting Agenda, Project Kick-Off Meeting Briefing and Project Kick-Off Meeting Minutes.

Deliverable:

A. Project Kick-Off Meeting Agenda
B. Project Kick-Off Meeting Briefing
C. Project Kick-Off Meeting Minutes

5.1.2 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a CPMP that lays out the Contractor's approach, installation schedule, and tools to be used in execution of the contract. The CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon and updated monthly thereafter. The Contractor shall update and maintain the VA PM approved CPMP throughout the period of performance.

Deliverable:

A. Contractor Project Management Plan

5.1.3 REPORTING REQUIREMENTS

The Contractor shall provide the COR with Monthly Progress Reports in electronic form in Microsoft Word and Project formats. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding month.

The Monthly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

The Contractor shall participate in a weekly teleconference with the COR to review progress status and discuss any pending issues.

Deliverable:

A. Monthly Progress Report

5.2 ENVIRONMENTAL CONTROL UNITS

The contractor shall provide an environmental control unit (ECU) that has the following capabilities. Minimum capabilities should resemble the Autonome Environmental Care Unit or equivalent device with salient characteristics as follows:

1. ECU Core Unit:
   a. At least 4 GB RAM
   b. At least 80 GB Solid State Drive
   c. Windows 7 or latest version operating system
   d. Touch screen
   e. Can be programmed to perform no fewer than 150 functions
   f. Full on-board programming, no tools or hardware required
   g. Built-in infrared capture
   h. Macros (scenes) fully editable with up to 20 functions per macro
   i. Removed
   j. User-adjustable volume, brightness, and scan rate
   k. Custom template design functions
   l. Minimum of 12.1" LED touchscreen
   m. Minimum of 6-7 hour battery life
   n. Seamless File Backup & Management
   o. One Button Press Design for Remote Support Team Tools
   p. Remote Assistance
   q. Wi-Fi / Dual Mode Bluetooth 4.0 capabilities
   r. 4 USB Ports (minimum 2.0)
   s. 1 1394a Firewire Port
   t. 1 Headphone/1 Microphone jack 1/8"
   u. Integrated Universal Infrared Remote Capabilities with learning window and multiple IR emitters
   v. Integrated Z-Wave capability for environmental control utilization
   w. Dual switch ports for ancillary access equipment
   x. Assistive Technology software designed for application integration and multiple access methodologies
   y. Ability to mount the device to a bed as well as a wheelchair if necessary
   z. Minimum of 120 square foot coverage range
2. Voice Recognition and Control
   a. Input
      1) Speech
      2) Dual switch or single switch with scanning
      3) At least 96 unique and different words available with multiple command use
      4) Internal microphone
      5) External keys for caregiver use
   b. Output

1) Internal Loudspeaker
2) Auditory – provide voice feedback on menu commands that will acknowledge confirmation on a patient's voice command.
3) Additional ECU Accessories

3. Lamp Module that will control lamps of 40 to 300 watts
4. Head Controlled Mouse
    a. Operating Wave Band: Near Infrared
    b. Capable of Wireless Operation
    c. Power Consumption: 1 Watt, minimum
    d. Field of view: At least 45-degrees by 60-degrees
    e. Standard Target: At least 0.25 inch (6.5mm) Diameter
    f. Measurement Rate: 45 Hz
    g. Measurement Latency: 10 msec.
5. Joints for articulating arms shall allow for a minimum of 180 degree of rotation on any axis.
6. Base for mounting arms shall have the ability to transfer locations
7. ECU shall be capable of being controlled by eye gaze with the following characteristics:
    a. Tracking – Hybrid infrared video eye & binocular & monocular tracking
    b. Working volume – minimum of 300x200x200mm3 (WxHxD)
    c. Accuracy, static - 0.5 degree
    d. Accuracy, over full working volume – 1 degree
8. ECU shall be capable of being controlled by sip n' puff tubing and straws that are commercially available
9. ECU shall have single and dual switch scanning
10. ECU shall provide access and interfaces to utilize computer games, E-books, ability to write documents, internet access and social video networking applications
    a. Privacy speaker port and Pillow speaker with privacy equivalent to that of a privacy speaker
    b. Wall bracket that is compatible with the dual mounting for televisions
12. ECU shall interface with nurse call systems to include, but not limited to, the following:
    a. Rauland Responder 5
    b. Rauland Responder 4
    c. Hill Rom Nurse Model # MCMMP5
13. All cabling required to interface with the hospital equipment shall be included, including:
    a. Nurse Call cables with ¼" male jacks to 1/8" jacks, cables 20ft in length
    b. Switch Cables from ECU device to bed unit
    c. Additional bed cables will be determined by bed type. Bed type will be verified in field.
14. Compatible with the following bed types to include, but not limited to,:
    a. Stryker: GoBed+, Gobed 2, Secure 2, Patriot.
    b. Hill Rom: Care Assist Bed Models, Advanta 350, Flexicare II, Versacare, Clinitron bed, Rite Hite bed (Clinitron half tub), and Rite Hite Air Fluidized Therapy bed.
15. Mounting for the sip-n-puff straws, microphones, speakers, and other accessories must be included for the beds. If a facility owned bed is not available, a portable cart modified for the mounting must be provided. The cart must meet the following characteristics:
    a. Locking wheels
    b. A minimum size work surface of 500 square inches
    c. Weight capacity of 150 lbs
    d. Height adjustable from 27.5" – 37.5"

16. Augmentative communication capabilities to include word prediction software must also be included.

17. Ability to delete user settings and saved documents in between patients must be included.
18. Break away cable with a single connection for control by patient care providers (bed)
19. Cable management to include cable coverings and protection (bed)
20. Software interface for ECU capable of being minimized for full PC features by administrative staff
21. Dual mounting to accommodate any existing arm-mounted patient televisions that will be encountered during installation of the ECUs. The contractor shall transfer existing patient televisions being provided as Government Furnished Property (GFP) to the new dual mount and for the installation of ECUs. Minimum capabilities for the custom dual mount shall resemble the PDi Communication System Mod PD168-046 Dual Monitor Mount or equivalent device with salient characteristics as follows:
    1. The mounting for the televisions shall be designed to be dual mounting and support both the weight of the television as well as the weight of the environmental control unit.
    2. The mounting bracket shall be able to rotate approximately 300 degrees and have +/- 15 degrees of tilt towards and away from the patient in order to accommodate special needs of patients.
    3. The arm for the mounting shall have a channel for nurse call.
    4. An external channel shall be supplied on the outside of the arm for the cabling for the environmental control unit.
    5. Installation at every patient bed in the spinal cord unit shall minimize disruption to patient care.

The Contractor shall warrant that the products they install shall be free from defects in materials and workmanship for a period of no less than two years from the date of acceptance. If any such product proves defective during the warranty period the vendor will repair the defective product at no charge to the Government for parts and labor, or a replacement in exchange for the defective product.

5.3 BASE PERIOD ECUS

The Contractor shall provide environmental control units as described in paragraph 5.2 above to the following locations:

Deliverables:

A. ECUs for 89 beds at James A. Haley VAMC, Tampa, FL
B. ECUs for 27 beds at Louis Stokes VAMC, Cleveland, OH

5.3.1 SITE KICKOFF MEETING

The Contractor shall participate in a Site Kick-off Meeting (SKM) to be held 30 days after contract award. The purpose of the SKM for each individual site is to ensure that there is an understanding between VA and the Contractor of the work to be executed at the site, the project approach, major actions, the schedule for key milestones and deliverables, and what is needed from VA and the Contractor to ensure project success. The Contractor shall provide a SKM Briefing which shall review task coordination details, schedules and topics, deliverable review and issue resolution processes and preferred site communication mechanisms at each site.

Deliverables:

A. Site Kick-Off Meeting Agenda for James A. Haley VAMC, Tampa, FL
B. Site Kick-Off Meeting Briefing for James A. Haley VAMC, Tampa, FL
C. Site Kick-Off Meeting Minutes for James A. Haley VAMC, Tampa, FL

D. Site Kick-Off Meeting Agenda for Louis Stokes VAMC, Cleveland, OH
E. Site Kick-Off Meeting Briefing for Louis Stokes VAMC, Cleveland, OH
F. Site Kick-Off Meeting Minutes for Louis Stokes VAMC, Cleveland, OH

5.3.2 ENVIRONMENTAL CONTROL UNIT INSTALLATION

The Contractor shall install an ECU in a single, non-occupied patient room in the spinal cord injury unit in order to work out the process for installation. Once completed, the Contractor shall coordinate with biomedical engineering and nursing staff to install all remaining ECU's in patient rooms. In the event the regular bed is not available or is replaced with a temporary substitute, the contractor shall provide portable cart with a height adjustable from 27.5" to 37.5" high, locking wheels and a work surface available for mounting of flexible arm with microphone, sip n' puff and components. In addition to the installation of the environmental control units, the arms and accessories such as the sip n puff straw, microphone will also be installed on all patient beds.

The entire system shall be installed and functional at the conclusion of the installation to include all accessories. The Contractor shall coordinate the installation schedule with the COR and facility Point of Contact (POC). The Contractor shall coordinate installations to occur at the same time with minimal disruption to the patients.

Deliverables:

A. ECU Installation at James A. Haley VAMC, Tampa, FL
B. ECU Installation at Louis Stokes VAMC, Cleveland, OH

5.3.3 ENVIRONMENTAL CONTROL UNIT CONFIGURATION

The Contractor shall ensure the configuration of all units includes environmental control system units along with command center conference phone with privacy speaker port, pillow speaker, mic input, microphone, direct IR input and wall mount bracket; Command Center Interface with IR relay, 4 way bed control, IR receiver, Nurse call, 3 IR emitter block, and Light module.

Placement of wall components shall be on a pre-assembled wall mounted panel to contain the telephone, sub command center and command center. This wall material shall have a standard requirement of 17" x 26" and shall have an area behind the panel to contain some wires if necessary.

From this panel shall be a cable leading to the bed called a "break away cable". This cable shall contain the bed control, privacy microphone, privacy speaker and sip and puff switch wires. The cable shall be in two pieces, with a disconnect capability within 2 to 4 feet from the bed to allow the nursing staff or others to detach the bed from the environmental control before moving the bed.

The Contractor shall provide an ECU Configuration report that details the installation and configuration of each ECU as it is configured.

Deliverable:

A. ECU Configuration and Report for James A. Haley VAMC, Tampa, FL
B. ECU Configuration and Report for Louis Stokes VAMC, Cleveland, OH

5.3.4 ENVIRONMENTAL CONTROL UNITS TESTING & ACCEPTANCE

The Government will accept the units upon Contractor demonstration and successful operation of the ECU for 10 calendar days. The demonstration shall include performance of the following:

Input (Access):

1. The user can effectively operate the available input (access) method described in the Performance Work Statement.
2. The input (access) method is reliable and repeatable.
3. The input (access) method has the capability to be modified to accommodate changes in the user's condition.

Ease of Learning:

1. The memory and sequencing requirements is user friendly.
2. The system can start with a single function and expand into a full system at a later time.
3. User functions can be excluded if necessary.

Multiple Control Base Sites:

The system has the capability to be operated from a wheelchair as well as from bed and from different rooms.

Feedback:

1. The user can adjust the ECU feedback to accommodate specific needs (e.g. vision or hearing problems).
2. Feedback reliable and recognizable.

Menu:

1. Choices are presented in an understandable way.
2. Homepage is accessible at all times.

Accessory Accommodation:

1. The system shall accommodate the addition of accessories to control additional functions if necessary.
2. The system can be customized to meet the unique needs of a specific user.
3. Battery backup is available.

Additional testing to be evaluated is as follows:

ECU:

1. Infrared distribution with a minimum reception range of up to 80 ft/24 m
2. At least 4 IR designer emitters
3. Full power bed control (head up and down, foot up and down)
4. A nurse-call interface
5. At least two (2) relays to interface with other automated devices such as door openers, light switches, etc.

Eye Gaze:

1. Tracking – Hybrid infrared video eye & binocular & monocular tracking
2. Working volume – minimum of 300x200x200mm3 (WxHxD)
3. Accuracy, static - 0.5 degree
4. Accuracy, over full working volume – 1 degree
5. Windows 7 or greater capability

Sip and Puff Straws:

Sip and Puff tubes shall contain Therafin or equivalent straw clear inner tubing and bacteria filters. Sip and Puff boxes shall include boxes and ports for auxiliary switches.

Head Mouse:

1. Operating Wave Band: Near Infrared
2. Capable of Wireless Operation
3. Power Consumption: 1 Watt, minimum
4. Field of view: At least 45-degrees by 60-degrees
5. Standard Target: At least 0.25 inch (6.5mm) Diameter
6. Measurement Rate: 45 Hz
7. Measurement Latency: 10 msec.

Deliverable:

A. Customer Acceptance Report- James A. Haley VAMC, Tampa, FL
B. Customer Acceptance Report- Louis Stokes VAMC, Cleveland, OH

5.3.5 CLINICIAN TRAINING

The Contractor shall develop and deliver train-the-trainer training during the site acceptance period to clinicians on the use of the Environmental Control Units. The goal of the clinician training will be to allow them to train the patients in the operation of the ECU and bedside television. The training for clinicians shall include a review of the ECU Quick start Guide, User operating manuals, handouts, and hands-on training to cover all of the ECU functionality. The training sessions shall be approximately four hours in duration and have a maximum class size of four clinicians per session.
The number of personnel to be trained at each facility is identified below.

1. James A. Haley VAMC- 13 Clinicians
2. Louis Stokes VAMC – 13 Clinicians

Deliverables:

A. Clinician Training - James A. Haley VAMC - 13 Clinicians

B. Clinician Training - Louis Stokes VAMC – 13 Clinicians

C. Clinician Training Material (Quick Start Guide, User Manual and handouts used during training) - James A. Haley VAMC - 3 Clinicians

D Clinician Training Material (Quick Start Guide, User Manual and handouts used during training) - Louis Stokes VAMC – 13 Clinicians

5.3.6 TECHNICIAN TRAINING

The Contractor shall develop and deliver a separate training session for site selected technician personnel on troubleshooting and maintaining the equipment during the site acceptance period. This course shall contain all the material (ECU Quick start Guide, User operating manuals, handouts) provided in the clinician training and additional information on trouble shooting and maintenance procedures. The technician user guide shall contain the necessary schematics and part lists for the VA to maintain the equipment after the expiration of the Contractor's warranty period. The training session shall not exceed four hours in duration.

The number of personnel to be trained at each facility is identified below.

1. James A. Haley VAMC – 3 Technicians

2. Louis Stokes VAMC – 3 Technicians
3. Michael E. DeBakey VAMC – 3 Technicians
4. James J. Peters VAMC – 3 Technicians

Deliverables:

A. Technician Training - James A. Haley VAMC - 3 Technicians

B. Technician Training - Louis Stokes VAMC – 3 Technicians

C. Technician Training Material (Quick Start Guide, User Manual, Maintenance and Troubleshoot Guide and handouts used during training) - James A. Haley VAMC - 3 Technicians

D. Technician Training Material - (Quick Start Guide, User Manual, Maintenance and Troubleshoot Guide and handouts used during training) - Louis Stokes VAMC – 3 Technicians

5.4 OPTION PERIOD ONE

The Contactor shall participate in SKM for option period one sites as detailed in PWS paragraph 5.3.1 and provide CPMP monthly updates and monthly reports as detailed in PWS paragraphs 5.1.2 through 5.1.3.

5.4.1 ECU

The Contractor shall provide environmental control units as described in paragraph 5.2 above to the following locations:

Deliverables:

A. ECUs for 11 beds at VA Long Beach Healthcare System, Long Beach, CA
B. ECUs for 13 beds at VA Palo Alto Healthcare System, Palo Alto, CA
C. ECUs for 6 beds at VA Saint Louis Health Care System, St. Louis, MO
D. ECUs for 2 beds at VA San Diego Health Care System, San Diego, CA
E. ECUs for 64 beds at Hampton VAMC, Hampton, VA
F. 3 Rolling Carts Modified for Bed Items at Hampton VAMC, Hampton, VA

5.4.2 ECU INSTALLATION

The Contactor shall work with biomedical engineering and nursing staff to install ECU's in patient rooms. In addition to the installation of the environmental control units, the arms and accessories such as the sip n puff straw, microphone, etc. will also be installed on all patient beds. The entire system will be installed and functional at the conclusion of the installation to include all accessories. This will be coordinated to occur with minimal disruption to the patients.

Deliverables:

A. ECU Installation at VA Long Beach Healthcare System
B. ECU Installation at VA Palo Alto Healthcare System
C. ECU Installation at VA Saint Louis Health Care System
D. ECU Installation at VA San Diego Health Care System
E. ECU Installation at Hampton VAMC

5.4.3 ECU CONFIGURATION

Configuration of all units includes environmental control system units along with command center conference phone with privacy speaker port, pillow speaker, mic input, microphone, direct IR input and wall mount

bracket; Command Center Interface with IR relay, 6 way bed control, IR receiver, Nurse call, 3 IR emitter block, and Light module.

Placement of wall components to be on a pre-assembled wall mounted panel to contain the telephone, sub command center and command center. This wall material will have a standard requirement of 12" x 24" and will have an area behind the panel to contain some wires if necessary.

From this panel will be a cable leading to the bed called a "break away cable". This cable will contain the bed control, privacy microphone, privacy speaker and sip and puff switch wires. The cable will be in two pieces, with a disconnect capability within 2 to 4 feet from the bed to allow the nursing staff or others to detach the bed from the environmental control before moving the bed.

The Contractor shall provide an ECU Configuration Report that details the installation and configuration of each ECU as it is configured.

Deliverable:

A. ECU Configuration and Reports for VA Long Beach Healthcare System
B. ECU Configuration and Reports for VA Palo Alto Healthcare System
C. ECU Configuration and Reports for VA Saint Louis Health Care System
D. ECU Configuration and Reports for VA San Diego Health Care System
E. ECU Configuration and Reports for Hampton VAMC

5.4.4 ACCEPTANCE AND TESTING

The Government will accept the units installed and configured in Option Period Two upon demonstration of their ability to perform each of the requirements detailed in section 5.2 above.

Deliverable:

A. Customer Acceptance Report 11 beds at VA Long Beach Healthcare System
B. Customer Acceptance Report 13 beds at VA Palo Alto Healthcare System
C. Customer Acceptance Report 6 beds at VA Saint Louis Health Care System
D. Customer Acceptance Report 2 beds at VA San Diego Health Care System
E. Customer Acceptance Report 64 beds at Hampton VAMC

5.4.5 CLINICIAN TRAINING

The Contractor shall provide training to clinicians on use of the Environmental Control Units at each site as described in 5.3.6. The number of personnel to be trained at each facility is identified below.

1. VA Long Beach Healthcare System, Long Beach, CA – 13 Clinicians
2. VA Palo Alto Healthcare System, Palo Alto, CA – 13 Clinicians
3. VA Saint Louis Health Care System, Saint Louis, MO– 13 Clinicians
4. VA San Diego Health Care System, San Diego, CA – 13 Clinicians
5. Hampton VAMC, Hampton, VA– 13 Clinicians

Deliverables:

A. Clinician Training - VA Long Beach Healthcare System – 13 Clinicians

B. Clinician Training - VA Palo Alto Healthcare System – 13 Clinicians
C. Clinician Training - VA Saint Louis Health Care System – 13 Clinicians
D. Clinician Training - VA San Diego Health Care System – 13 Clinicians
E. Clinician Training - Hampton VAMC – 13 Clinicians
F. Clinician Training Material (Quick Start Guide, User Manual and handouts used during training) - VA Long Beach Healthcare System – 13 Clinicians
G. Clinician Training Material (Quick Start Guide, User Manual and handouts used during training) -VA Palo Alto Healthcare System – 13 Clinicians
H. Clinician Training Material (Quick Start Guide, User Manual and handouts used during training) - VA Saint Louis Health Care System – 13 Clinicians
I. Clinician Training Material (Quick Start Guide, User Manual and handouts used during training) -VA San Diego Health Care System – 13 Clinicians
J. Clinician Training Material (Quick Start Guide, User Manual and handouts used during training) - Hampton VAMC – 13 Clinicians

5.4.6 TECHNICIAN TRAINING

The Contractor shall provide training to Technicians on use of the Environmental Control Units at each site as described in 5.3.7. The number of personnel to be trained at each facility is identified below.

1. VA Long Beach Healthcare System, Long Beach, CA – 3 Technicians
2. VA Palo Alto Healthcare System, Palo Alto, CA – 3 Technicians
3. VA Saint Louis Health Care System, Saint Louis, MO– 3 Technicians
4. VA San Diego Health Care System, San Diego, CA – 3 Technicians
5. Hampton VAMC, Hampton, VA– 3 Technicians

Deliverables:

A. Technician Training - VA Long Beach Healthcare System – 3 Technicians
B. Technician Training - VA Palo Alto Healthcare System – 3 Technicians
C. Technician Training - VA Saint Louis Health Care System – 3 Technicians
D. Technician Training -VA San Diego Health Care System – 3 Technicians
E. Technician Training – Hampton VAMC – 3 Technicians
F. Technician Training Material (Quick Start Guide, User Manual, Maintenance and Troubleshoot Guide and handouts used during training) - VA Long Beach Healthcare System – 3 Technicians
G. Technician Training Material (Quick Start Guide, User Manual, Maintenance and Troubleshoot Guide and handouts used during training) -VA Palo Alto Healthcare System – 3 Technicians
H. Technician Training Material (Quick Start Guide, User Manual, Maintenance and Troubleshoot Guide and handouts used during training) -VA Saint Louis Health Care System – 3 Technicians
I. Technician Training Material (Quick Start Guide, User Manual, Maintenance and Troubleshoot Guide and handouts used during training) -VA San Diego Health Care System – 3 Technicians
J. Technician Training Material (Quick Start Guide, User Manual, Maintenance and Troubleshoot Guide and handouts used during training) –Hampton VAMC – 3 Technicians

6.0 GENERAL REQUIREMENTS

6.1 GENERAL REQUIREMENTS FOR INSTALLATION OF DEVICES AND CUSTOM MOUNTING

A) The Contractor shall completely prepare site for removal and installation of equipment. The Contractor shall furnish all labor and materials and perform work as required by specifications.

B) All employees of the Contractor and their Subcontractors shall comply with VA security management program.

C) Restoration:

The Contractor shall clean up all work areas after completing work in VA facilities; repair any damages including removal and disposal of defective equipment. The contractor shall immediately repair and/or replace all facilities and/or equipment damaged by the contractor and/or their subcontractors. All areas affected shall be restored to their original condition. The contractor shall include a Damage Incident log in their monthly progress report submitted to the Government detailing any damages as well as their restoration activities and completion

D) Final Cleanup: Upon completion of the project, or as work progresses, The Contractor shall remove all installation debris that has been part of the installation.

6.2 POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

6.3 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Security Suitability Program," Appendix A)
Low	**National Agency Check with Written Inquiries (NACI)** A NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Security Suitability Program," Appendix A)
Moderate	**Moderate Background Investigation (MBI)** A MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High	**Background Investigation (BI)** A BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the Performance Work Statement are:

	Position Sensitivity and Background Investigation Requirements		
Task Number	Low/NACI	Moderate/MBI	High/BI
5.1	☒	☐	☐
5.2	☒	☐	☐
5.3	☒	☐	☐
5.4	☒	☐	☐

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

6.4 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.

b. The Contractor shall bear the expense of obtaining background investigations.

c. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations. The roster shall contain the Contractor's Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement (based upon Section 6.2 Tasks).

d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.

e. For a Low Risk designation the following forms are required to be completed: 1.OF-306 and 2. DVA Memorandum – Electronic Fingerprints. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710 and 2. DVA Memorandum – Electronic Fingerprints. These should be submitted to the COR within 5 business days after award.

f. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC), through the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). The Contractor personnel shall submit all required information related to their background investigations utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).

g. The Contractor is to certify and release the e-QIP document, print and sign the signature pages, and send them to the COR for electronic submission to the SIC. These should be submitted to the COR within 3 business days of receipt of the e-QIP notification email.

h. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.

i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).

j. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.

k. Failure to comply with the Contractor personnel security investigative requirements may result in termination of the contract for default.

6.5 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.6 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Performance Levels for Objectives associated with this effort**.**

Contractor performance will be measured in terms of timely performance of tasks and the level of quality being provided by the contractor. Examples representing timeliness and quality may include Monthly Report Delivery (Monthly reports are delivered on time 80% of the time); error rate (no more than 3 issues omitted from a monthly report; 100% of the time). These represent an acceptable level of performance.

Performance Objective	Performance Standard	Acceptable Performance Levels
1. Technical Needs	Shows understanding of requirements Efficient and effective in meeting requirements Meets technical needs and mission requirements Offers quality services/products	Satisfactory or higher
2. Project Milestones and Schedule	Quick response capability Products completed, reviewed, delivered in timely manner Notifies customer in advance of potential problems	Satisfactory or higher
3. Project Staffing	Currency of expertise Personnel possess necessary knowledge, skills and abilities to	Satisfactory or higher

	perform tasks	
4. Value Added	Provided valuable service to Government Services/products delivered were of desired quality	Satisfactory or higher

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable manner. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion.

6.7 FACILITY/RESOURCE PROVISIONS

The VA shall provide electrical utilities at wall locations and quad outlets as needed.

The VA shall provide the cable signal to the televisions as required by having the cable pulled and ready for connection to each television in the project.

The VA facility shall provide a climate controlled secure room for the contractor to store materials and work, located in the nearby area of the work to be accomplished.

The Government will provide office space, telephone service and system access when authorized contract staff work at a Government location as required in order to accomplish the Tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the COR as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

VA will provide access to VA specific systems/network as required for execution of the task via remote access technology (e.g. Citrix Access Gateway (CAG), site-to-site VPN, or VA Remote Access Security Compliance Update Environment (RESCUE)). This remote access will provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses. The Contractor shall utilize Government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. For detailed Security and Privacy Requirements refer to ADDENDUM A and ADDENDUM B.

6.8 GOVERNMENT FURNISHED PROPERTY

The Government will existing patient televisions for the Contractor to mount on dual mounts in conjunction with the installation of ECUs.

ADDENDUM A

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the Project Manager, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

Each documented initiative under this contract incorporates VA Handbook 6500.6, "Contract Security," March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), and will be tracked therein. The TMS may be accessed at https://www.tms.va.gov. If you do not have a TMS profile, go to https://www.tms.va.gov and click on the "Create New User" link on the TMS to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance**.**

A2.1. VA Internet and Intranet Standards:

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but

is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed are published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

Section 508 – Electronic and Information Technology (EIT) Standards:

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http://www.section508.gov and http://www.access-board.gov/sec508/standards.htm. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

_x_ § 1194.21 Software applications and operating systems
_x_ § 1194.22 Web-based intranet and internet information and applications
_x_ § 1194.23 Telecommunications products
_x_ § 1194.24 Video and multimedia products
_x_ § 1194.25 Self contained, closed products
_x_ § 1194.26 Desktop and portable computers
_x_ § 1194.31 Functional Performance Criteria
_x_ § 1194.41 Information, Documentation, and Support

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

A4.0 Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.

2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.

3. Smoking is prohibited inside/outside any building other than the designated smoking areas.

4. Possession of weapons is prohibited.

5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

2. The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.

3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.

4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA Contracting Officer.

5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.

6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.

7. Contractor must adhere to the following:

    a. The use of "thumb drives" or any other medium for transport of information is expressly prohibited.

    b. Controlled access to system and security software and documentation.

    c. Recording, monitoring, and control of passwords and privileges.

    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.

    e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.

    f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.

g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".

h. Contractor does not require access to classified data.

8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.

ADDENDUM B

APPLICABLE PARAGRAPHS TAILORED FROM: *THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE, VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010*

B1. GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The Contracting Officer must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way

without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

8. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

9. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA minimum requirements. VA Configuration Guidelines are available upon request.

10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

B4. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be reviewed and approved by VA prior to implementation.

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the Contractor's systems in accordance with VA Handbook 6500.3, *Certification and*

Accreditation and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

e. The Contractor/Subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

1) Vendor must accept the system without the drive;

2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;

a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

B5. SECURITY INCIDENT INVESTIGATION

a. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B6. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract.

b. The Contractor/Subcontractor shall provide notice to VA of a "security incident" as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

1) Nature of the event (loss, theft, unauthorized access);

2) Description of the event, including:

a) date of occurrence;

b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

3) Number of individuals affected or potentially affected;

4) Names of individuals or groups affected or potentially affected;

5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

6) Amount of time the data has been out of VA control;

7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

8) Known misuses of data containing sensitive personal information, if any;

9) Assessment of the potential harm to the affected individuals;

10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and

11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification;

2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;

3) Data breach analysis;

4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;

5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and

6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B7. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

B8. TRAINING

a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems;

2) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* training and annually complete required security training;

3) Successfully complete *Privacy and HIPAA Training* if Contractor will have access to PHI;

4) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

5) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access

b. The Contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.